

Amendments to the Claims:

This listing of claims will replace, without prejudice, all prior versions, and listings, of claims in the application:

Listing of Claims:

1. – 58. Cancelled.

59. (New) A system for remote access of an environment comprising:
an Internet browser connectable to an extranet;
an extranet located external to said environment and accessible via said Internet browser;
at least one communications server located in said extranet and adapted to interconnect on-demand with one of a series of connection gateways located in predetermined environments; and
a connection gateway located in said environment ;
wherein upon accessing a predetermined address by said Internet browser on said extranet, said communications server subsequently creates a new connection to a predetermined one of said connection gateways to control or monitor the operation of at least one service in said environment, with said connection gateway subsequently providing access to information contained within the environment directly to said Internet browser.

60. (New) A system as claimed in claim 59 where in the connection gateway located in said environment is adapted to serve a user interface for the control or monitoring of the operation of at least one service in said environment.

61. (New) A system as claimed in claim 60 wherein said service is adapted to monitor or control, one or more devices interconnected with said connection gateway.

62. (New) A system as claimed in claim 60 wherein said service is adapted to monitor and control, one or more devices interconnected with said connection gateway.

63. (New) A system as claimed in claim 61, wherein at least one of said devices is a monitoring device located within said environment.

64. (New) A system as claimed in claim 59, wherein said communication server utilises a telecommunications network to interconnect with said connection gateway.

65. (New) A system as claimed in claim 59, wherein authentication to access said extranet is required only once per Internet browser session.

66. (New) A system as claimed in claim 59, wherein said extranet forms part of the Internet and said communications server is located within the local telephone call radius of the environment, thus providing lowest cost PSTN access from or to the environment.

67. (New) A system as claimed in claim 59, wherein additional interface pages accessible via said browser are provided on said extranet for each user of said system, said pages adaptable to provide details of the current status of the environment of said user.

68. (New) A system as claimed in claim 59, wherein said extranet provides a user premises e-mail facility, and automatically raises connection in a pre-programmed fashion to said connection gateway and transfers user e-mail to said connection gateway.

69. (New) A system as claimed in claim 59, wherein said Internet browser runs on an Internet access device which includes a smart card reader and associated user smart card which provides authentication details and URL corresponding to said environment.

70. (New) A system as claimed in claim 69, wherein said smart card also facilitates global access to the Internet for access of said extranet, and optionally additionally tracks connections for expenses.

71. (New) A system as claimed in claim 69, wherein the Internet access device is a computer, WebPhone, Portable digital assistant, or mobile phone with web browsing capability.

72. (New) A system as claimed in claim 59, wherein the connection gateway detects a fax and stores the fax.

73. (New) A system as claimed in claim 59, wherein the connection gateway is in a tamper proof enclosure, and operates without mains power.

74. (New) A system as claimed in claim 59, wherein the connection gateway is tamper proof, and triggers an alarm and relays alarm to the provider network in case of attempted tampering.

75. (New) A system as claimed in claim 61, wherein the connection gateway acts as a hub and Internet connection mechanism for connected devices including information appliances and said devices located in said environment.

76. (New) A system as claimed in claim 59, further comprising a control terminal interconnected to said connection gateway.

77. (New) A system as claimed in claim 76, wherein the control terminal is equipped with biosensor, for access authentication of a local user in said environment to said connection gateway.

78. (New) A system as claimed in claim 75, wherein the control terminal is connected to said connection gateway in a wireless manner.

79. (New) A system as claimed in claim 78, wherein the control terminal is powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to the user premises network in said environment.

80. (New) A system as claimed in claim 76, wherein control terminal is of reduced handheld size, so that can operate as universal premises remote control.

81. (New) A system as claimed in claim 76, wherein the control terminal includes a digital camera, microphone and speaker, and video conferencing software, thus allowing the control terminal to be used as a videophone, through a standard browser interface.

82. (New) A system as claimed in claim 76, wherein a control terminal includes a personal computer (PC) equipped with a user premises network connection, wherein said PC runs a browser accessing a URL corresponding to said connection gateway.

83. (New) A system as claimed in claim 76, wherein the control terminal is provided by set top box connected to a television and running a web browser.

84. (New) A system as claimed in claim 76, wherein said control terminal is equipped with a smartcard reader for e-commerce transactions over said extranet.

85. (New) A system as claimed in claim 76, wherein at least one of said devices comprises a digital security camera embodying image capture and compression method and an interconnection to said connection gateway.

86. (New) A system as claimed in claim 85, wherein said camera includes motion detection and image significance algorithms which run in said camera, and filter input so that only detected motion input is compressed and sent through said connection gateway to said extranet.

87. (New) A system as claimed in claim 59, wherein said connection gateway provides support for at least one of the HomePnP, Bluetooth, HomeRF, Hiperlan or HAVi standard for network communication and appliance control.

88. (New) A system as claimed in claim 59, wherein said connection gateways form nodes of a distributed computing environment that may be allocated by said extranet on a demand basis.

89. (New) A system as claimed in claim 59, for providing information access across at least two networks, wherein:

said extranet is a first network having a first network access controller; and

said environment is a second network having a second network access controller;

said system further comprising a user access browser located on said first network for locating and examining information on said first and second networks by means of network address locators;

wherein when a predetermined location on said network is accessed, said first network access controller initiates the establishment of a network connection to said second network access controller so as to provide for the temporary interconnection of said first network to said second network, said system thereby providing a seamless access to information stored on said second network from said user access browser.

90. (New) A system as claimed in claim 89, wherein said network address locators comprise Universal Resource Locators.

91. (New) A system as claimed in claim 59 for monitoring an environment, said system further comprising:

storage means forming part of said extranet; and
a device activating a security condition upon the occurrence of a predetermined event;
wherein, upon the occurrence of said predetermined event, said device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for later interrogation by a user of said system and initiates predetermined alert notification actions .

92. (New) A system as claimed in claim 91, wherein said device includes alert conditions which are forwarded to said connection gateway, wherein it is qualified with a pre-programmed enable, and if the result is TRUE, an event is generated, whereupon said connection gateway establishes a connection with one of said communications servers

93. (New) A system as claimed in claim 92 wherein said device is a security sensor device, said system is a security system, said event is a security alarm event, and said data is surveillance data or security alert data.

94. (New) A system as claimed in claim 93, wherein surveillance data related to said alarm event is uploaded to said extranet for secure storage accessible upon interrogation by a user.

95. (New) A system as claimed in claim 92, wherein photos of authorised occupants of said environment are accessible from said extranet and are accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised.

96. (New) A system as claimed in claim 92 wherein the connection gateway incorporates a user programmed phone call answer strategy, including delayed answer, and upon answering said phone call, optionally detects a voice call, in which case it records a compressed version of the voice call for later retrieval by the user, thus operating in answering machine mode.

97. (New) A system as claimed in claim 96, wherein upon answering an incoming call, the connection gateway raise a connection to a communications server, and sends an indication to the user of said security system of the receipt of a recorded message.

98. (New) A system as claimed in claim 92, wherein said connection gateway sends a recorded compressed voice messages to a communications server for storage on said extranet for forwarding to a user of said environment.

99. (New) A system as claimed in claim 92, wherein the connection gateway provides an indication of messages received on a HTML page accessible by a user of said home environment.

100. (New) A system as claimed in claim 92, wherein said connection gateway is programmable to allow different response mechanisms to differing classes of alert event.

101. (New) A system as claimed in claim 92, wherein said connection gateway contains connection details for preferred and secondary communication servers on said extranet, so that if a first communication server does not respond, other communication servers may be contacted until successful connection is achieved.

102. (New) A system as claimed in claim 92, wherein user data storage on said extranet for storing event data associated with said environment is allocated virtually.

103. (New) A system as claimed in claim 92, wherein said user data storage on said extranet is allocated redundantly, ensuring integrity of stored surveillance data.

104. (New) A system as claimed in claim 92, wherein said extranet includes a user contact database which includes preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of e-mail, pager, computer generated voice message through telephone, requesting response, or after a specified timeout has elapsed, security action.

105. (New) A system as claimed in claim 92, wherein at least one of said devices includes an external access control mechanism to said environment.

106. (New) A system as claimed in claim 92, wherein at least one of said devices includes a reader for an RF tag embodied in keyfob or other device that is used for user authentication.

107. (New) A system as claimed in claim 92, wherein at least one of said devices includes a smartcard reader that is used for user authentication.

108. (New) A system as claimed in claim 107, wherein the smartcard includes a biosensor attached to the substrate of the smart card and interconnected with a circuit embedded in smartcard to authenticate user before the smartcard will operate.

109. (New) A system as claimed in claim 59, where said environment is a home environment.

110. (New) A system as claimed in claim 59, where said environment is a commercial environment.

111. (New) A system as claimed in claim 59, where said environment is an industrial environment.

112. (New) A system as claimed in claim 59, wherein the at least one service includes a security monitoring service.

113. (New) A system as claimed in claim 59, wherein the at least one service includes a video surveillance service.

114. (New) A system as claimed in claim 59, wherein the at least one service includes an automation and control service.

115. (New) A system as claimed in claim 59, wherein the at least one service includes a utility metering service.

116. (New) A system as claimed in claim 59, wherein the at least one service includes an energy management service.

117. (New) A system as claimed in claim 59, where service implements monitoring or control of a plurality of devices connected to at least one network interconnected with connection gateway.

118. (New) A system as claimed in claim 59, where the Internet browser is on a mobile phone.

119. (New) A system as claimed in claim 59, wherein said the Internet browser runs on an Internet access device which includes a smart card reader and associated user smart

card which provides authentication to access said predetermined address to create a connection to said environment.

120. (New) A system as claimed in claim 91, wherein the connection gateway is embodied in a security camera.

121. (New) A security system for monitoring an environment comprising:
an extranet located external to said environment;
storage means forming part of said extranet;
at least one communications server located in said extranet and adapted to interconnect on demand with one of a series of connection gateways located in predetermined environments;

a connection gateway located in said environment adapted to control or monitor the operation of at least one security device in said environment; and

a device activating an alert condition upon the occurrence of a predetermined event; wherein, upon the occurrence of said predetermined event, said device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for remote storage for later interrogation by a user of said security system and initiates predetermined alert notification actions.

122. (New) A system as claimed in claim 121, wherein the connection gateway is tamper proof, and triggers an alarm and relays alarm to the provider network in case of attempted tampering.